Configureer de instellingen van Simple Network Management Protocol (SNMP) op een RV34x Series router

Doel

Simple Network Management Protocol (SNMP) wordt gebruikt voor netwerkbeheer, probleemoplossing en onderhoud. SNMP registreert, slaat en deelt informatie met de hulp van twee zeer belangrijke software: een netwerkbeheersysteem (NMS) dat op beheerapparaten en een agent die op beheerde apparaten draait. De RV34x Series router ondersteunt SNMP versies 1, 2 en 3.

SNMP v1 is de oorspronkelijke versie van SNMP die bepaalde functionaliteit ontbeert en alleen werkt op TCP/IP-netwerken, terwijl SNMP v2 een verbeterde iteratie van v1 is. SNMP v1 en v2c mogen alleen worden gekozen voor netwerken die SNMPv1 of SNMPv2c gebruiken. SNMP v3 is de nieuwste standaard van SNMP en behandelt veel problemen van SNMP v1 en v2c. Het gaat met name in op veel van de veiligheidskwetsbaarheden van v1 en v2c. SNMP v3 stelt beheerders ook in staat om naar één gemeenschappelijke SNMP-standaard te verplaatsen.

Dit artikel legt uit hoe u SNMP-instellingen kunt configureren op de RV34x Series router.

Toepasselijke apparaten

- RV34x Series

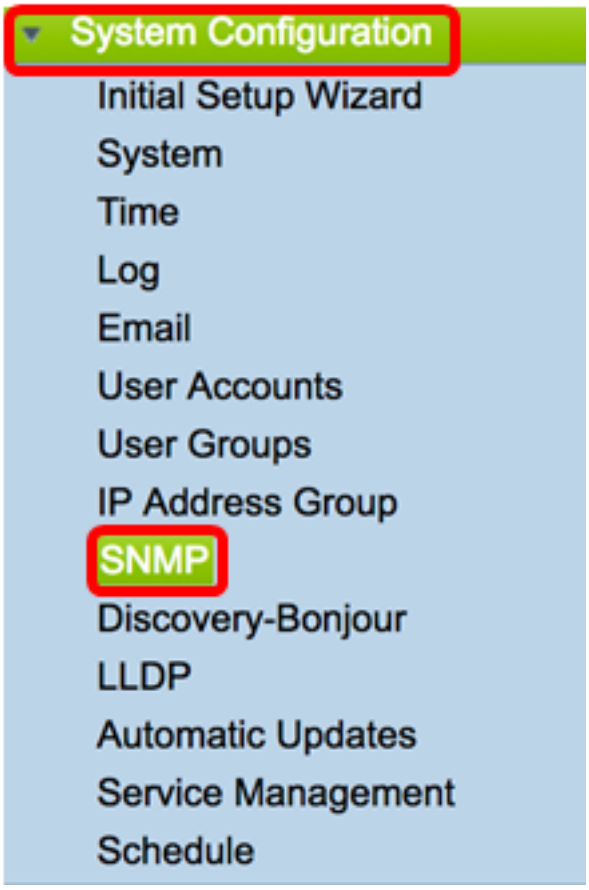
Softwareversie

- 1.0.1.16

SNMP-instellingen configureren op RV34x Series router

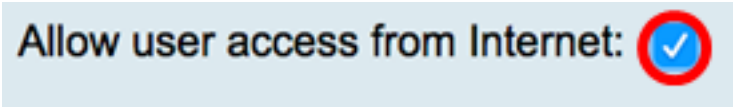
SNMP-instellingen configureren

Stap 1. Meld u aan bij het op web gebaseerde hulpprogramma van de router en kies **Systeemconfiguratie > SNMP**.

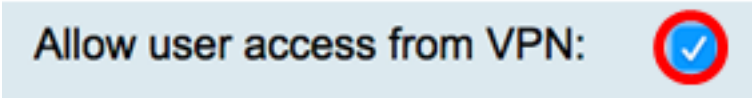


Stap 2. Controleer het aanvinkvakje **SNMP inschakelen** om SNMP in te schakelen.

Stap 3. (Optioneel) Controleer het aanvinkvakje **Toegang voor gebruiker vanaf internet** toestaan om geautoriseerde gebruikers toegang tot het netwerk te bieden via beheertoepassingen zoals Cisco FindIT Network Management.



Stap 4. (Optioneel) Controleer het aanvinkvakje **Toegang voor gebruiker via VPN** om geautoriseerde toegang van een VPN mogelijk te maken.

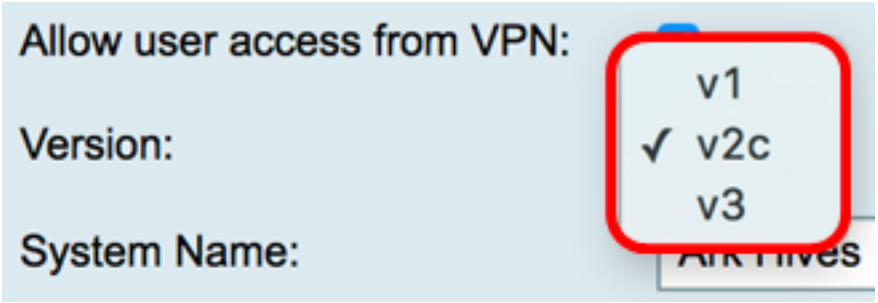


Stap 5. Kies een SNMP-versie die u in het uitrolmenu van de versie wilt gebruiken. De opties zijn:

- v1 — Minimaal verzekerde optie. Gebruikt kladtekst voor community strings.
- v2c — De verbeterde ondersteuning voor foutenbehandeling van SNMPv2c omvat uitgebreide foutcodes die verschillende soorten fouten onderscheiden; alle soorten fouten worden door één foutcode in SNMPv1 gerapporteerd.
- v3 — SNMPv3 is een veiligheidsmodel waarin een authenticatiestrategie wordt opgezet voor een gebruiker en de groep waarin de gebruiker verblijft. Beveiligingsniveau is het toegestane

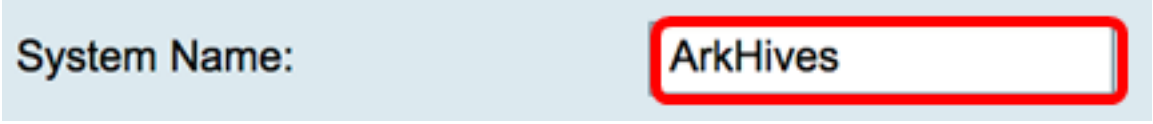
veiligheidsniveau binnen een beveiligingsmodel. Een combinatie van een beveiligingsmodel en een beveiligingsniveau bepaalt welk beveiligingsmechanisme wordt gebruikt bij de verwerking van een SNMP-pakket.

Opmerking: In dit voorbeeld wordt v2c gekozen.



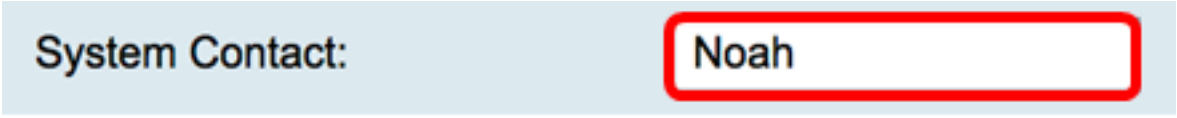
Stap 6. In het veld *Systeemnaam* typt u een naam voor de router voor makkelijke identificatie in netwerkbeheertoepassingen.

Opmerking: In dit voorbeeld wordt ArkHives gebruikt als de systeemnaam.



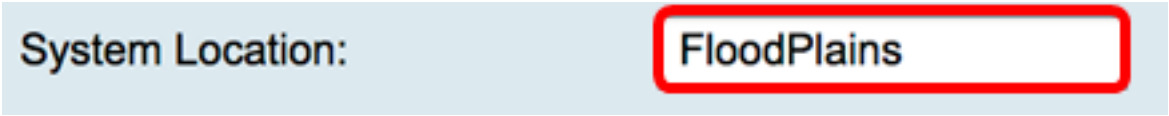
Stap 7. In het veld *System Contact*, typt u een naam van een persoon of beheerder om zich in geval van een noodgeval te identificeren met de router.

Opmerking: Dit voorbeeld, Noah wordt gebruikt als het Systeemcontact.



Stap 8. Voer in het veld *Systeemlocatie* een locatie van de router in. Dit maakt de lokalisatie van een probleem veel gemakkelijker voor een beheerder.

Opmerking: Bij dit voorbeeld wordt FloodPlains gebruikt als de systeemlocatie.



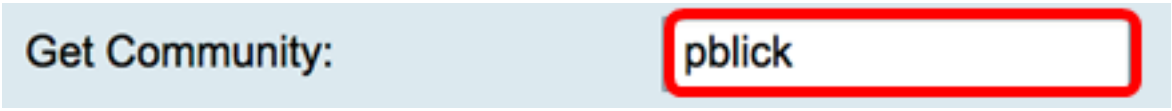
Klik met de configuratie op de SNMP-versie die in Stap 5 is geselecteerd.

- SNMP 1 of v2c configureren
- SNMP v3 configureren

SNMP 1 of v2c configureren

Stap 1. Als SNMP v2c in Stap 5 is geselecteerd, voert u de SNMP-community-naam in het veld *Get Community*. Het creëert een alleen-lezen gemeenschap die wordt gebruikt om de informatie voor SNMP agent te gebruiken. De community string die wordt verstuurd in het aanvraagpakket dat door zender wordt verstuurd moet overeenkomen met de community string op het agent apparaat. De standaard string voor alleen-lezen is openbaar.

Opmerking: Het alleen-lezen wachtwoord geeft alleen autoriteit om informatie op te halen. In dit voorbeeld wordt pblick gebruikt.



Stap 2. Voer in het veld *Community-set*, een SNMP-community-naam in. Het creëert een read-Writcommunity die wordt gebruikt om toegang te krijgen tot de informatie voor SNMP-agent. Alleen verzoeken van de hulpmiddelen die zich met deze gemeenschapsnaam identificeren worden aanvaard. Dit is een door de gebruiker gemaakte naam. Het standaard is privé.

Opmerking: Het is raadzaam beide wachtwoorden in een meer aangepast patroon te wijzigen om beveiligingsaanvallen van buitenstaanders te voorkomen. In dit voorbeeld wordt pribado gebruikt.

U hebt nu met succes de SNMP v1- of v2-instellingen ingesteld. Ga verder naar het gebied Trap Configuration.

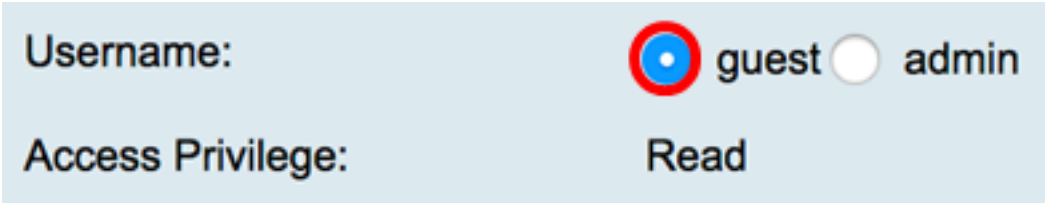
SNMP v3 configureren

Stap 1. Als SNMP v3 is geselecteerd, klikt u op een radioknop in het gebied Naam om een toegangsvoorrecht te kiezen. De opties zijn:

- gast — Lees-only privileges
- beheerder — Lees- en schrijfrechten

Opmerking: Voor dit voorbeeld wordt de gast gekozen.

Het gebied van het Voorrecht van de Toegang toont het type van voorrecht afhankelijk van de klikte radioknop.



Stap 2. Klik een radioknop in het gebied Verificatiealgoritme om een methode te kiezen die de SNMP agent zal gebruiken om te authentiseren. De opties zijn:

- Geen — Er wordt geen gebruikersverificatie gebruikt.
- MD5 — Message-Digest Algorithm 5 gebruikt een hashwaarde van 128 bits voor verificatie. Vereist naam en wachtwoord.
- SHA1 - Secure Hash Algorithm (SHA-1) is een eenrichtinggevend algoritme dat een 160-bits vertering produceert. SHA-1 compileert langzamer dan MD5, maar is veiliger dan MD5.

Opmerking: In dit voorbeeld wordt MD5 geselecteerd.

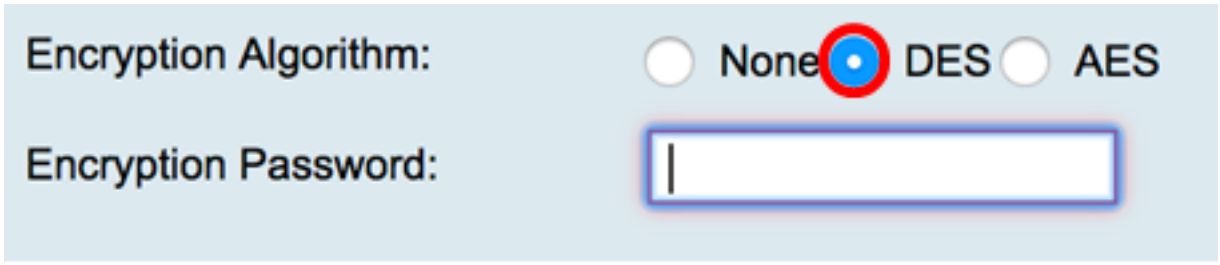
Opmerking: Als u geen heeft gekozen, gaat u naar het gebied Trap Configuration.

Stap 3. Voer in het veld *Wachtwoord* voor verificatie in.

Stap 4. (Optioneel) Klik in het gebied Encryption Algorithm op een radioknop om te kiezen hoe SNMP-informatie moet worden versleuteld. De opties zijn:

- Geen — Er wordt geen encryptie gebruikt. Als deze stap is geselecteerd, slaat u de stekker over naar het gebied Trap Configuration.
- DES — Data Encryption Standard (DES) is een 56-bits coderingsmethode die niet erg veilig is, maar vereist is voor compatibiliteit met de achterzijde.
- AES — Advanced Encryption Standard (AES). Als dit is geselecteerd, is een coderingswachtwoord vereist.

Opmerking: Bijvoorbeeld, DES wordt gekozen.



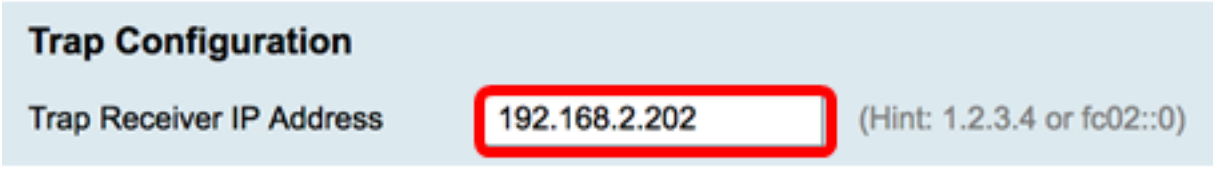
Stap 5. (Optioneel) Als DES of AES is geselecteerd, typt u een encryptiewachtwoord in het veld *Encryption Password*.

U dient nu met succes de SNMP v3-instellingen te hebben configureren. Ga nu naar het gebied Trap Configuration.

Vlagconfiguratie

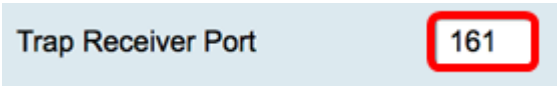
Stap 1. Voer in het veld *IP-adres van de* ontvanger *van de* trap een IPv4- of IPv6-adres in dat de SNMP-trap zal ontvangen.

Opmerking: Voor dit voorbeeld wordt 192.168.2.2002 gebruikt.

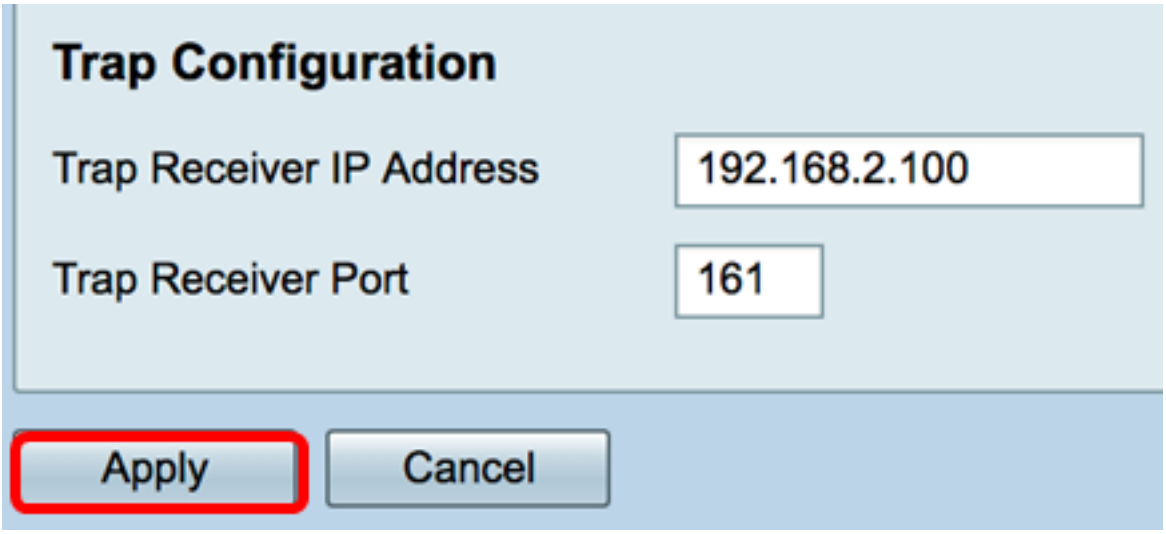


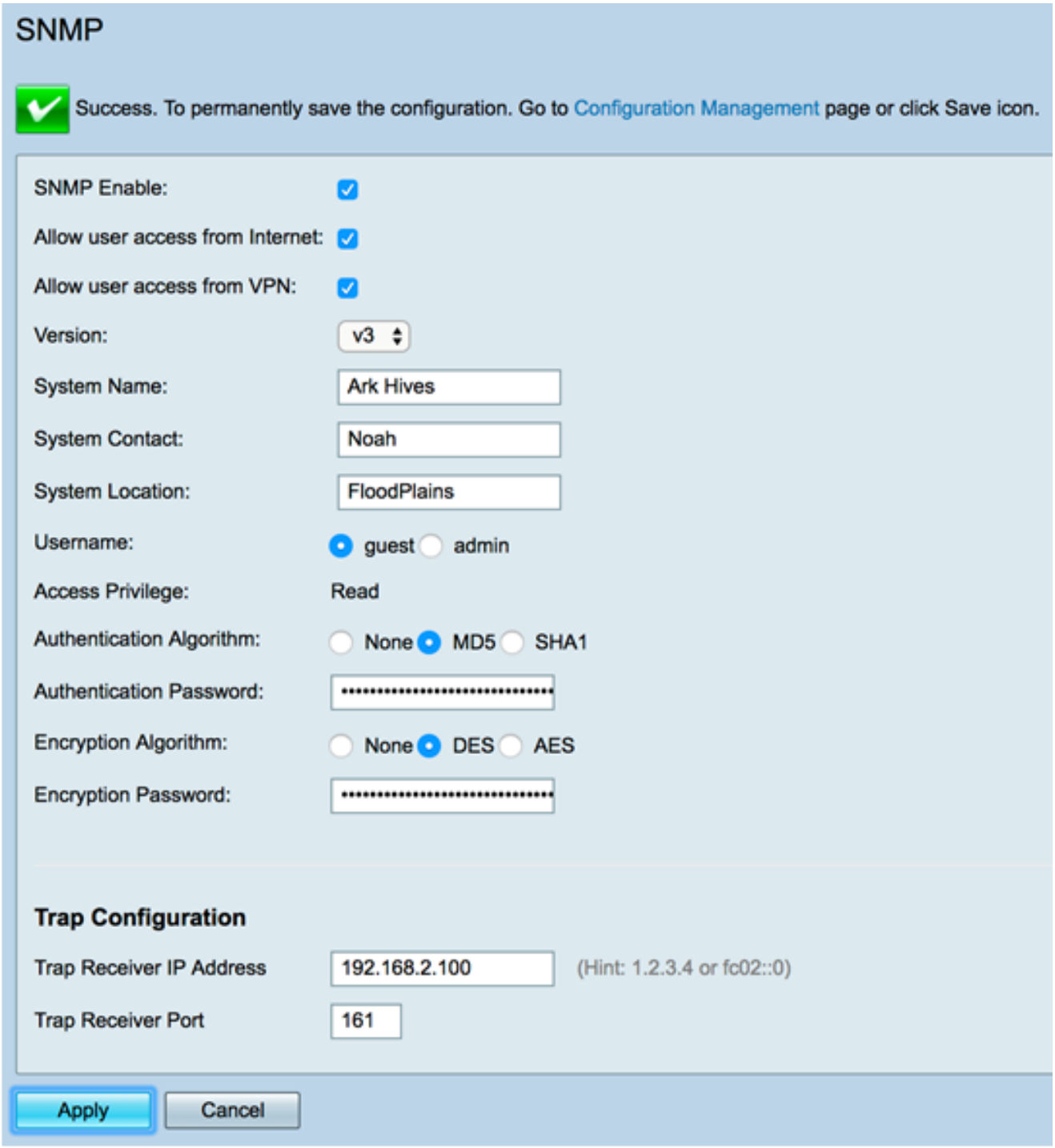
Stap 2. Voer een UDP-poortnummer (User Datagram Protocol) in in het veld *Trap ontvangerpoort*. De SNMP agent controleert deze poort voor toegangsverzoeken.

Opmerking: Voor dit voorbeeld wordt 161 gebruikt.



Stap 3. Klik op **Toepassen**.





Stap 4. (Optioneel) Om de configuratie permanent op te slaan, gaat u naar de pagina Configuratie kopiëren/opslaan of klikt u op het 

pictogram in het bovenste gedeelte van de pagina.

U dient nu met succes de SNMP-instellingen te hebben ingesteld op een RV34x Series router.